EMA SECURITY

Yönetilen MDR ve SOC Hizmeti

AI-Powered Defense Service

İletişim

www.emasecurity.com

info@emasecurity.com

Bostancı Mah, Ali Nihat Tarhan Cd, Kahraman Sk,
No:2/D:11, Hoffman Plaza, Kadıkoy/İstanbul

+90 (850) 244 49 26

Hizmet Tanımı

MDR (Managed Detection and Response) ve SOC (Security Operations Center) hizmetleri, kuruluşların siber güvenlik tehditlerine karşı proaktif, sürekli ve hızlı yanıt verebilmesini sağlayan yönetilen güvenlik çözümleridir. Geleneksel güvenlik önlemleri, gelişen tehdit vektörleri ve sofistike saldırılar karşısında yetersiz kalabilirken, MDR ve SOC hizmetleri, organizasyonlara gerçek zamanlı tehdit tespiti, olay yönetimi ve müdahale yetenekleri kazandırarak güvenlik süreçlerini daha etkin hale getirir.

MDR Hizmeti: MDR, tehditlerin tespiti ve analiz edilmesinin ötesinde, tehdit avcılığı (threat hunting) ve proaktif müdahale süreçlerini içeren yönetilen bir siber güvenlik hizmetidir. Yapay zeka destekli analitikler, makine öğrenimi algoritmaları ve büyük veri analizi kullanarak anomali tespiti yapar, güvenlik olaylarını ilişkilendirir ve saldırıları erken aşamada belirleyerek riskleri minimize eder. MDR hizmeti, gelişmiş tehdit modelleme tekniklerini kullanarak MITRE ATT&CK çerçevesine uygun saldırı tespitleri yapar ve organizasyonların siber tehditlere karşı hazırlıklı olmasını sağlar.

SOC Hizmeti: SOC, organizasyonların 7/24 izlenen merkezi güvenlik operasyonlarını yöneten ve tehditlere karşı hızlı müdahale edilmesini sağlayan bir güvenlik operasyon merkezidir. SOC ekipleri, SIEM (Security Information and Event Management) sistemleri ile büyük hacimli güvenlik olaylarını analiz eder, tehdit istihbaratı kaynaklarını entegre eder ve saldırılara karşı anlık yanıt verilmesini sağlar. SOC süreçleri, log yönetimi, anomali tespiti, adli bilişim analizi, tehdit istihbaratı analizi ve otomatik müdahale mekanizmaları gibi kritik güvenlik bileşenlerini kapsar.

MDR ve SOC Entegrasyonu: MDR ve SOC hizmetleri birlikte çalışarak organizasyonların güvenlik operasyonlarını daha kapsamlı ve etkili hale getirir. MDR hizmeti, SOC ekipleri tarafından yönetilen güvenlik olaylarını daha derinlemesine analiz eder ve saldırganların yöntemlerini belirleyerek organizasyonların korunmasını sağlar. SOAR (Security Orchestration, Automation and Response) entegrasyonu sayesinde tehditlere karşı otomatik aksiyon alınarak saldırıların daha başlamadan engellenmesi sağlanır.

Hizmete Ait Bileşenler

Tehdit İstihbaratı Entegrasyonu

MDR ve SOC hizmetleri, tehdit aktörlerinin taktik, teknik ve prosedürlerini (TTP) belirlemek için açık kaynak tehdit istihbaratı (OSINT), ticari istihbarat sağlayıcıları ve özel tehdit analizleri ile entegre çalışır.

Sürekli Güvenlik İzleme

Güvenlik olayları, uç noktalardan, ağlardan, bulut ortamlarından ve kritik sistemlerden 7/24 izlenir. SIEM (Security Information and Event Management) çözümleri ile korelasyon kurularak anormal aktiviteler tespit edilir.

Anomali Tespiti ve Davranış Analitiği

Yapay zeka (AI) ve makine öğrenimi (ML) destekli sistemlerle kullanıcı ve varlık davranış analitiği (UEBA) gerçekleştirilir. Olağandışı aktiviteler tespit edilerek tehdit seviyeleri değerlendirilir.

Olay Yanıt ve Müdahale (Incident Response)

Tespit edilen tehditlere karşı otomatik ve manuel müdahale mekanizmaları devreye sokulur. NIST 800-61 çerçevesine uygun olarak olay inceleme, izolasyon, tehdit yok etme ve iyileştirme süreçleri yürütülür.

Tehdit Avcılığı (Threat Hunting)

Pasif güvenlik önlemlerinin ötesine geçilerek, tehdit istihbaratı ve geçmiş olay analizleri kullanılarak proaktif tehdit avcılığı yapılır. SOC ekipleri, saldırganların varlığını erken aşamada tespit ederek zararı en aza indirir.

SOAR (Security Orchestration, Automation, and Response) Entegrasyonu

Güvenlik olaylarının hızlı ve etkili bir şekilde yönetilmesini sağlamak için SOAR çözümleri kullanılır. Otomatik aksiyonlarla tehditlere karşı daha hızlı yanıt verilir.

Zararlı Yazılım Analizi ve Adli Bilişim (Forensics & Malware Analysis)

Tespit edilen tehditlerin kaynakları analiz edilir, zararlı yazılımlar tersine mühendislik teknikleriyle incelenir ve olay sonrası adli bilişim çalışmaları yürütülerek saldırganların izleri takip edilir.

Ağ ve Uç Nokta Güvenliği (Network & Endpoint Security)

EDR (Endpoint Detection and Response) ve NDR (Network Detection and Response) çözümleri ile uç noktalardan ve ağdan gelen veriler analiz edilerek tehditlere karşı aktif koruma sağlanır.

Uyumluluk ve Raporlama

MDR ve SOC hizmetleri, KVKK, ISO 27001, GDPR ve NIST gibi regülasyonlara uygun olarak güvenlik raporlaması yapar. Güvenlik duruşu ve olay analizleri düzenli olarak organizasyona sunularak şeffaflık sağlanır.

Mevcut Durum Analizi

MDR ve SOC hizmetleri uygulanmadan önce kuruluşun mevcut güvenlik altyapısı detaylı bir şekilde incelenir. Kullanılan SIEM (Security Information and Event Management) sistemleri, uç nokta güvenlik çözümleri, olay müdahale süreçleri ve tehdit algılama mekanizmaları değerlendirilerek, organizasyonun tehditlere karşı dayanıklılığı analiz edilir. Bu analiz sonucunda güvenlik açıkları tespit edilerek, en kritik zafiyetlerin önceliklendirildiği bir yol haritası oluşturulur.

Strateji ve Yol Haritası Belirleme

MDR ve SOC hizmetlerinin uygulanmasına yönelik strateji, kuruluşun büyüklüğüne, faaliyet alanına ve mevcut risk seviyesine göre belirlenir. SOC ekibinin 7/24 izleme, tehdit analizi ve olay müdahale süreçlerini nasıl yürüteceği detaylandırılırken, MDR hizmetleri kapsamında uygulanacak tehdit avcılığı, tehdit istihbaratı entegrasyonu ve otomatik yanıt mekanizmaları planlanır. Ayrıca, SOC süreçlerinin iç kaynaklarla mı yoksa yönetilen hizmet sağlayıcılar aracılığıyla mı yürütüleceği belirlenerek en uygun operasyonel model tasarlanır.

MDR ve SOC Uygulama Aşamaları

SOC hizmeti kapsamında ilk olarak güvenlik olaylarının izlenmesi için SIEM ve SOAR çözümleri devreye alınır. Anomali tespiti için makine öğrenmesi destekli tehdit analitik sistemleri kurularak, log yönetimi ve olay korelasyonu süreçleri güçlendirilir. MDR hizmeti kapsamında, tehdit avcılığı (Threat Hunting) çalışmaları yürütülerek, proaktif tehdit tespiti yapılır ve olası saldırılara karşı önleyici aksiyonlar alınır. Güvenlik olaylarının yanıtlama süresi en aza indirilerek, otomatik müdahale mekanizmaları geliştirilir. SOC ve MDR entegrasyonu sayesinde, saldırılar daha hızlı tespit edilerek, olaylara anında yanıt verilir ve sistemlerin güvenliği sürekli olarak sağlanır.

MDR ve SOC Uygulama Metodolojisi

MDR ve SOC hizmetlerinin başarılı bir şekilde uygulanması için Gartner tarafından önerilen güvenlik çerçeveleri ve NIST 800-61 olay müdahale kılavuzları temel alınarak kapsamlı bir metodoloji izlenir. İlk aşamada, kuruluşun tüm bilgi sistemlerinden, uç noktalardan, ağ cihazlarından, bulut hizmetlerinden ve güvenlik çözümlerinden gelen büyük hacimli veriler toplanarak analiz edilir. Bu süreçte, güvenlik olaylarına ait günlük kayıtları (loglar), ağ trafiği verileri, tehdit istihbaratı kaynakları ve uç nokta güvenliği çözümlerinden elde edilen bilgiler kullanılır. Toplanan veriler, yapay zeka ve makine öğrenimi algoritmaları ile analiz edilerek, normal sistem ve kullanıcı davranışları belirlenir ve anormal aktiviteler tespit edilir. Olası tehditler, MITRE ATT&CK çerçevesine göre bilinen saldırı teknikleriyle karşılaştırılarak saldırı girişimleri belirlenir. Tespit edilen tehditlere yönelik müdahale planları hızla uygulanarak, saldırganların kullanabileceği güvenlik açıkları kapatılır ve saldırı vektörleri ortadan kaldırılır. SIEM ve SOAR entegrasyonu sayesinde, güvenlik olaylarına otomatik yanıt verilir ve tehditlerin yayılması önlenir. Bununla birlikte, sürekli güncellenen tehdit istihbaratı sayesinde MDR ve SOC hizmetleri dinamik olarak optimize edilir, yeni saldırı tekniklerine karşı adaptasyon sağlanır ve organizasyonun güvenlik duruşu sürekli olarak iyileştirilir.

Raporlama ve İyileştirme

MDR ve SOC hizmetleri kapsamında, tespit edilen tehditler, saldırı girişimleri ve alınan aksiyonlar detaylı olarak raporlanır. Güvenlik operasyonlarının etkinliği ölçülerek, iyileştirme alanları belirlenir. Olay sonrası analiz çalışmaları gerçekleştirilerek, gelecekte benzer saldırıların önlenmesi için güvenlik politikaları güçlendirilir. Yönetim seviyesinde sunulan özet raporlarla, karar vericilere siber güvenlik stratejileri hakkında kapsamlı bilgiler sağlanır. Bu süreç, sürekli izleme ve optimizasyon ile kurumun güvenlik olgunluğunu artırmayı hedefler.

Sıkça Sorulan Sorular (SSS)

MDR ve SOC arasındaki fark nedir?

SOC, güvenlik olaylarını izleyen ve analiz eden bir operasyon merkezidir, MDR ise proaktif tehdit avcılığı, analiz ve müdahale hizmetleri sunarak tehditlere karşı anlık yanıt verir.

MDR ve SOC hizmetleri tüm sektörlere uygun mudur?

Evet, finans, sağlık, kamu, e-ticaret ve üretim gibi çeşitli sektörlerde uygulanabilir ve sektöre özel tehdit modelleri geliştirilerek optimize edilebilir.

SOC hizmeti iç kaynaklarla mı yoksa dış kaynaklarla mı yürütülmelidir?

Bu, organizasyonun büyüklüğüne ve teknik kapasitesine bağlıdır. Küçük ve orta ölçekli işletmeler için yönetilen SOC hizmetleri (SOC as a Service) daha uygun olabilirken, büyük kuruluşlar kendi SOC operasyonlarını kurmayı tercih edebilir.

MDR hizmetleri manuel mi yoksa otomatik mi çalışır?

MDR hizmetleri hem manuel tehdit avcılığı hem de otomatik olay tespiti ve yanıtlama mekanizmaları içerir. Yapay zeka destekli sistemlerle süreçler hızlandırılır.

MDR ve SOC hizmetleri mevcut güvenlik sistemleriyle entegre edilebilir mi?

Evet, SIEM, EDR/XDR, güvenlik duvarları, IPS/IDS ve diğer güvenlik çözümleri ile entegre çalışarak kuruluşun mevcut güvenlik altyapısını tamamlar ve güçlendirir.

MDR hizmeti fidye yazılımlarına (ransomware) karşı koruma sağlar mı?

Evet, MDR hizmeti fidye yazılım saldırılarını önlemek için gelişmiş tehdit tespiti, EDR/XDR çözümleri ve otomatik yanıt mekanizmaları ile koruma sağlar. Anormal davranışları tespit ederek kötü amaçlı yazılımların yayılmasını engeller.